UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

RICHARD DUSTERHOFT, et al,

Plaintiffs,

v. Case No. 22-cv-0882-bhl

ONETOUCHPOINT CORP,

Defendant.

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS

This putative class action stems from an April 2022 data breach in which hackers gained access to Defendant OneTouchPoint Corp. (OneTouchPoint)'s computer systems. Plaintiffs have filed fifteen lawsuits against OneTouchPoint, alleging that their personal information was exposed as a result of the data breach. In a September 29, 2022 order, the Court consolidated the actions and appointed interim co-lead counsel, who, with OneTouchPoint's consent, filed a Consolidated and Amended Class Action Complaint (Consolidated Complaint). (See ECF Nos. 12 & 15.) After the parties spent more than a year attempting a settlement, on November 20, 2023, OneTouchPoint filed a motion to dismiss, contending that Plaintiffs lack standing to pursue their claims and, even if they have standing, they fail to state actionable claims. (ECF Nos. 55 & 55-1.)

The Court will grant OneTouchPoint's motion but only in part. With respect to standing, the Court is skeptical that all of the named Plaintiffs have in fact suffered sufficiently concrete injuries to support standing, but under binding Seventh Circuit law, the Consolidated Complaint sufficiently alleges injury at the pleading stage for all but one Plaintiff (Dusterhoft). The Court agrees with OneTouchPoint, however, that Plaintiffs' claims for injunctive and declaratory relief are unlikely to be redressed by a favorable decision and that portion of the motion to dismiss will be granted. The Court also agrees with OneTouchPoint that Plaintiffs have failed to support at least some of their substantive claims with plausible factual allegations sufficient to maintain those claims, and those claims will be dismissed. Plaintiffs have adequately alleged several of their other claims, however, and OneTouchPoint's motion will be denied as to those causes of action, which

include their common-law claims for negligence, negligence per se, and unjust enrichment, as well as statutory claims under Wisconsin, Georgia, and South Carolina law.

BACKGROUND[1]

This litigation arises from an April 27, 2022 data breach at OneTouchPoint. (ECF No. 15 ¶5.) OneTouchPoint is a mailing and printing services vendor in the healthcare sector. (*Id.* ¶2.) Plaintiffs include patients of OneTouchPoint's clients whose personal information was compromised in the data breach, along with two former OneTouchPoint employees whose information was similarly compromised. (*Id.* ¶¶43, 208, 278.) Plaintiffs' proposed class includes the approximately 2.6 million individuals whose personal information was exposed during the breach. (*Id.* ¶¶1, 22.)

OneTouchPoint is a Delaware corporation headquartered in Hartland, Wisconsin. (*Id.* ¶33.) It provides services including brand management, marketing, printing, and supply chain logistics to healthcare providers. (*Id.* ¶37.) In order to provide its services, OneTouchPoint requires its clients to provide information about their patients, including personally identifiable information (PII) and personal health information (PHI). (*Id.* ¶¶1, 3.) The information OneTouchPoint collects and maintains includes names, addresses, Social Security numbers (SSNs), member IDs, dates of birth, health insurance information, and other medical information provided during health assessments. (*Id.* ¶¶3, 39.)

On April 28, 2022, OneTouchPoint detected encrypted files on some of its computer systems. (*Id.* ¶4.) A subsequent investigation revealed that an unauthorized party had accessed some of its servers on April 27, 2022. (*Id.* ¶5.) Less than six weeks later, on June 3, 2022, OneTouchPoint provided written notice of the breach to its clients. (*Id.* ¶6.) The notice letter stated that "the impacted systems contained information related to individuals provided by [OneTouchPoint's] customers," but OneTouchPoint could not confirm what personal information was accessed by the perpetrator. (*Id.* ¶7.) OneTouchPoint initially reported that the breach impacted 1,073,316 individuals' data, but that number later rose to more than 2.6 million. (*Id.* ¶9.) The affected individuals include patients of nearly 40 health insurance companies and healthcare service providers. (*Id.* ¶60.)

[1] This Background is derived from Plaintiffs' Consolidated Complaint, (ECF No. 15), the allegations in which are presumed true when considering a motion to dismiss. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 554–56 (2007).

The scope of information compromised in the breach included names, member IDs, and information provided during health assessments including dates and descriptions of service, diagnosis codes, medications, medical recommendations, and other medical information. (*Id.* ¶10.) At least one OneTouchPoint client reported that SSNs were also exposed by the breach. (*Id.* ¶59.) In July 2022, OneTouchPoint began to provide written notice to individuals whose data was compromised in the breach. (*Id.* ¶54.)

Plaintiff Michael Meza is an Arizona resident and former OneTouchPoint employee. (*Id.* ¶¶24, 208.) He provided personal information to OneTouchPoint pursuant to his employment. (*Id.* ¶209.) In an August 26, 2022 letter, OneTouchPoint informed Meza that his personal information, including his name, SSN, and driver's license number, had been exposed in the breach. (*Id.* ¶210.) The letter advised him to "remain vigilant against incidents of identity theft and fraud by reviewing [his] account statements and monitoring free credit reports for suspicious activity." (*Id.*) OneTouchPoint offered Meza twelve months of complimentary credit monitoring and identity protection services through Equifax. (*Id.*) As a result of the breach, Meza has spent approximately two to three hours updating passwords and credits cards and anticipates spending more time and money to mitigate the effects of the data breach. (*Id.* ¶¶214, 217.)

Plaintiff Michael Meeks is a Georgia resident whose health insurance provider is Humana, a OneTouchPoint client. (*Id.* ¶¶25, 218.) Meeks provided personal information to Humana and Humana provided that information to OneTouchPoint. (*Id.* ¶219.) In a July 27, 2022 letter, OneTouchPoint informed Meeks that his personal information, including his name, member ID, and information he may have provided during a health assessment, had been exposed in the breach. (*Id.* ¶220.) Meeks was advised by OneTouchPoint to protect against fraud and identity theft but was not offered any complimentary credit monitoring. (*Id.*) Following the data breach, Meeks has experienced unauthorized charges from a credit company for a loan he did not apply for, as well as several bank notifications regarding loan payments for fraudulent loans. (*Id.* ¶224.) Meeks's credit score has also dropped 99 points following the breach and he has been informed that his SSN has been associated with an individual's employment at a hospital where Meeks has never worked. (*Id.*) Meeks has also noticed an increase in spam calls and texts following the breach. (*Id.*) He has spent several hours combating these issues and anticipates spending more time and money combatting the effects of the breach. (*Id.* ¶¶224, 227.)

Plaintiff Marcie Strickland is a Georgia resident whose health insurance provider is CareSource, a OneTouchPoint client. (*Id.* ¶¶26, 228.) Strickland provided personal information to CareSource and CareSource provided that information to OneTouchPoint. (*Id.* ¶229.) In a July 2022 letter, OneTouchPoint informed Strickland that her personal information, including her name, date of birth, address, member ID, and other medical information, had been exposed in the breach. (*Id.* ¶230.) Following the data breach, Strickland has experienced dozens of unauthorized credit inquiries that have impacted her ability to secure a home loan. (*Id.* ¶234.) She has also received an increase in spam calls, leading her to change her phone number. (*Id.*) Strickland has spent several hours responding to these incidents and anticipates spending more time and money combatting the effects of the breach. (*Id.* ¶¶234, 237.)

Plaintiff Richard Dusterhoft is a Minnesota resident who receives health insurance from Humana through Medicare. (*Id.* ¶¶28, 238.) Dusterhoft provided personal information to Humana and Humana provided that information to OneTouchPoint. (*Id.* ¶239.) In a July 27, 2022 letter, OneTouchPoint informed Dusterhoft that his personal information, including his name, member ID, and information he may have provided during a health assessment, had been exposed in the breach. (*Id.* ¶240.) Dusterhoft was advised by OneTouchPoint to protect against fraud and identity theft but was not offered any complimentary credit monitoring. (*Id.*) Following the data breach, Dusterhoft has received an increase in spam calls. (*Id.* ¶244.) Dusterhoft anticipates spending considerable time and money mitigating the effects of the breach. (*Id.* ¶247.)

Plaintiff Robin Guertin is a South Carolina resident whose health insurance provider is Humana. (*Id.* ¶¶29, 248.) Guertin provided personal information to Humana and Humana provided that information to OneTouchPoint. (*Id.* ¶249.) In a July 27, 2022 letter, OneTouchPoint informed Guertin that her personal information, including her name, member ID, and information she may have provided during a health assessment, had been exposed in the breach. (*Id.* ¶250.) Guertin was advised by OneTouchPoint to protect against fraud and identity theft but was not offered any complimentary credit monitoring. (*Id.*) As a result of the breach, Guertin has spent time carefully reviewing her accounts for fraudulent activity and anticipates spending more time and money to mitigate the effects of the data breach. (*Id.* ¶¶254, 257.)

Plaintiff Shira Haid is a Wisconsin resident whose health insurance provider is Common Ground Healthcare Cooperative (Common Ground), a OneTouchPoint client. (*Id.* ¶¶30, 258.) Haid provided personal information to Common Ground and Common Ground provided that

information to OneTouchPoint. (*Id.* ¶259.) In an August 2, 2022 letter, OneTouchPoint informed Haid that her personal information, including her name, address, date of birth, SSN, member ID, and other medical information, had been exposed in the breach. (*Id.* ¶260.) Haid was advised by OneTouchPoint to protect against fraud and identity theft but was not offered any complimentary credit monitoring. (*Id.*) Following the data breach, over $10,000 was fraudulently transferred from Haid's bank account. (*Id.* ¶264.) Haid has spent approximately 12 hours responding to this issue and anticipates spending more time and money combatting the effects of the breach. (*Id.* ¶¶264, 267.)

Plaintiff Aria Nardi is a Wisconsin resident whose health insurance providers at the time of the data breach were Common Ground and Anthem, both OneTouchPoint clients. (*Id.* ¶¶31, 268.) Nardi provided personal information to Common Ground and Anthem and they provided that information to OneTouchPoint. (*Id.* ¶269.) In an August 2, 2022 letter, OneTouchPoint informed Nardi that her personal information, including her name, address, date of birth, SSN, member ID, and other medical information, had been exposed in the breach. (*Id.* ¶270.) Nardi was advised by OneTouchPoint to protect against fraud and identity theft but was not offered any complimentary credit monitoring. (*Id.*) As a result of the breach, Nardi has spent approximately 1.5 hours proactively ensuring her financial security and anticipates spending more time and money to mitigate the effects of the data breach. (*Id.* ¶¶274, 277.)

Plaintiff Sheila Crosby is a Wisconsin resident and former OneTouchPoint employee. (*Id.* ¶¶32, 278.) She provided personal information to OneTouchPoint pursuant to her employment. (*Id.* ¶279.) In an August 26, 2022 letter, OneTouchPoint informed Crosby that her personal information, including her name, SSN, and financial information, had been exposed in the breach. (*Id.* ¶280.) OneTouchPoint offered Crosby 12 months of complimentary credit monitoring services. (*Id.*) Following the data breach, Crosby experienced several unauthorized charge attempts to her bank account. (*Id.* ¶284.) She has spent approximately 3 hours responding to these incidents and anticipates spending more time and money combatting the effects of the breach. (*Id.* ¶¶284, 287.)

Plaintiff Jeffrey Neil Young is a Maine resident who receives Medicare services from Martin's Point Health Care (Martin's Point). (*Id.* ¶¶27, 288.) Martin's Point is a customer of Matrix Medical Network (Matrix), which is a client of OneTouchPoint. (*Id.* ¶288.) Young provided personal information to Martin's Point and Matrix and they provided that information to

OneTouchPoint. (*Id.* ¶289.) In a July 28, 2022 letter, Martin's Point informed Young that his personal health information, including diagnoses, medication, and preventative and chronic care recommendations, had been exposed in the breach. (*Id.* ¶290.) Martin's Point offered Young free identity protection services through IDX. (*Id.* ¶291.) Following the breach, Young has repeatedly received spam and phishing texts, phone calls, and emails. (*Id.* ¶295.) Young has spent several hours dealing with these issues, as well as reviewing his credit card bills and credit reports for fraudulent activity. (*Id.*) Young anticipates spending considerable additional time and money combatting the effects of the breach. (*Id.* ¶299.)

Plaintiffs seek to certify a nationwide class of all individuals whose information was exposed in the data breach. (*Id.* ¶300.) Alternatively, or additionally, Plaintiffs seek to certify statewide classes of affected individuals in Arizona, Georgia, Maine, Minnesota, South Carolina, and Wisconsin, each of the six states in which a named plaintiff resides. (*Id.* ¶301.)

LEGAL STANDARD

Defendants invoke both Rule 12(b)(1) and 12(b)(6) in support of their motion to dismiss. "Rule 12(b)(1) is the means by which a defendant raises a defense that the court lacks subject-matter jurisdiction." *Bazile v. Fin. Sys. of Green Bay, Inc.*, 983 F.3d 274, 279 (7th Cir. 2020). Rule (12)(b)(1) motions often challenge the plaintiffs' standing, a doctrine that requires all plaintiffs to have a "personal stake" in the outcome of the case. *See id.*; *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021) (quoting *Raines v. Byrd*, 521 U.S. 811, 819 (1997)). Where a facial challenge to standing is made, the Court accepts the allegations in the complaint as true and draws all reasonable inferences in the plaintiffs' favor. *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 691 (7th Cir. 2015). Thus, to survive a facial challenge, plaintiffs must "clearly allege facts demonstrating" each element of standing. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)).

When deciding a Rule 12(b)(6) motion to dismiss, the Court must "accept all well-pleaded facts as true and draw reasonable inference in the plaintiffs' favor." *Roberts v. City of Chicago*, 817 F.3d 561, 564 (7th Cir. 2016) (citing *Lavalais v. Village of Melrose Park*, 734 F.3d 629, 632 (7th Cir. 2013)). A complaint will survive if it "state[s] a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

ANALYSIS

I. The Consolidated Complaint Adequately Pleads Facts Supporting Standing on Plaintiffs' Individual Claims for Damages but Not for Injunctive or Declaratory Relief.

Federal courts are courts of limited jurisdiction. Article III of the Constitution authorizes federal courts to exercise federal judicial power to decide "cases" and "controversies" within the jurisdiction authorized by Congress. *See* U.S. Const. art. III § 2. A plaintiff seeking to invoke a federal court's jurisdiction must have "standing" or a "personal stake" in the outcome of the case. *TransUnion*, 594 U.S. at 422 (quoting *Raines*, 521 U.S. at 819). To establish standing, a plaintiff must show: (1) an injury-in-fact; (2) that is fairly traceable to the defendant; and (3) likely to be redressed by a favorable judicial decision. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992). A plaintiff must establish standing for each claim asserted and each form of relief sought. *TransUnion*, 594 U.S. at 431 (citing *Davis v. Fed. Election Comm'n*, 554 U.S. 724, 734 (2008)). In the class action context, every class member must have standing to recover individual damages. *Id.*

The standing requirement exists at the inception of a case and continues through resolution. In other words, "[p]laintiffs must maintain their personal interest in the dispute at all stages of litigation." *Id.* (citing *Davis*, 554 U.S. at 733). The showing needed to establish standing varies at each stage of litigation "in the same way as any other matter on which the plaintiff bears the burden of proof." *Lujan*, 504 U.S. at 561. At the pleading stage, a defendant may move to dismiss for lack of standing under Rule 12(b)(1), at which point the Court accepts the allegations in the complaint as true and draws all reasonable inferences in the plaintiffs' favor, unless standing is challenged as a factual matter. *Remijas*, 794 F.3d at 691. Thus, to survive a facial Rule 12(b)(1) motion to dismiss, plaintiffs must "clearly allege facts demonstrating" each element of standing. *Spokeo*, 578 U.S. at 338 (quoting *Warth*, 422 U.S. at 518).

OneTouchPoint offers two facial challenges to Plaintiffs' standing allegations. First, it argues that five of the named Plaintiffs—Dusterhoft, Guertin, Meza, Nardi, and Young—lack standing because the Consolidated Complaint does not allege that any of them has suffered an injury-in-fact. (ECF No. 55-1 at 23–31.) Second, OneTouchPoint argues that all of the named Plaintiffs lack standing to request declaratory or injunctive relief from the Court because that relief is unlikely to redress their injuries. (*Id.* at 31–32.) In response, Plaintiffs insist that Dusterhoft, Guertin, Meza, Nardi, and Young have alleged injuries-in-fact resulting from their risk of identity

theft, time they have spent mitigating the effects of the breach, and the diminished value of their private information. (ECF No. 59 at 17–23.) Plaintiffs also argue that Plaintiffs have standing for declaratory and injunctive relief because the requested relief would protect them from an "imminent and substantial" risk that their private information is *again* exposed in *future* data breaches. (*Id.* at 23.)

A. Plaintiffs Guertin, Meza, Nardi, and Young Have Adequately Alleged Injury Based on Their Time Spent Mitigating the Effects of the Breach.

OneTouchPoint argues that Plaintiffs Dusterhoft, Guertin, Meza, Nardi, and Young lack standing to pursue their claims because they have not alleged to have suffered an injury-in-fact as a result of the data breach. (ECF No. 55-1 at 25–31.) "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560). An imminent and substantial risk of future harm is sufficient for the purposes of injunctive relief, *TransUnion*, 594 U.S. at 435, but "a risk of future harm, without more, is insufficiently concrete to permit standing to sue for damages in federal court." *Ewing v. MED-1 Sols., LLC*, 24 F.4th 1146, 1152 (7th Cir. 2022) (citing *TransUnion*, 594 U.S. at 436–37).

Plaintiffs insist that Dusterhoft, Guertin, Meza, Nardi, and Young have sufficiently alleged concrete injuries that support standing. More specifically, they point to allegations of three distinct injuries: (1) the impending and substantial risk of identity theft; (2) time spent mitigating their risks of potential identity theft; and (3) the diminution in value of their private information. (ECF No. 59 at 17.)

Plaintiffs' first theory of injury fails, even at the pleading stage. In *TransUnion*, the Supreme Court confirmed "that in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm." 594 U.S. at 436 (emphasis in original). That holding explicitly forecloses Plaintiffs' first theory. The mere risk of future identity theft is not a concrete harm in and of itself in a suit for damages. *See id.* at 441.

Plaintiffs' third injury theory also fails to support standing. The allegations concerning the diminution in the value of Plaintiffs' private information are too conclusory to support standing. Plaintiffs merely allege in conclusory fashion that they have suffered "damage to and diminution in the value of their Private Information, a form of property that [OneTouchPoint] obtained from Plaintiffs and Class Members." (ECF No. 15 ¶199.) But they offer no specific facts to support

any actual or concrete harm beyond this conjecture. Even at the pleading stage, conclusory allegations, unsupported by plausible facts, are insufficient to establish standing. *See Silha v. ACT, Inc.*, 807 F.3d 169, 174 (7th Cir. 2015). Plaintiffs rely on a handful of district court cases from other circuits that have concluded that diminution in the value of personal information is a concrete injury. (*See* ECF No. 59 at 21 (citing *In re Marriot Cust. Data Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783 (N.D. Cal. May 27, 2016); *Smallman v. MGM Resorts Int'l*, No. 2:20-cv-00376-GMN-EJY, 2022 WL 16636958 (D. Nev. Nov. 2, 2022).) But those cases are both factually distinct and unpersuasive. More importantly, the Seventh Circuit has rejected substantially similar arguments. *See Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 912–13 (7th Cir. 2017) (rejecting plaintiff's claim for deprivation of the economic value of his personal information as "gibberish"); *Silha*, 807 F.3d at 174–75 (concluding that plaintiffs were not harmed by defendant's sale of their personal information). Even in *Remijas* and *Lewert v. P.F. Chang's China Bistro, Inc.*, Seventh Circuit cases invoked by Plaintiffs, the court of appeals expressed disapproval of, without deciding, these same sorts of injuries as providing a basis for standing. *See Remijas*, 794 F.3d at 695; *Lewert*, 819 F.3d 963, 968 (7th Cir. 2016).

Plaintiffs' final theory of injury presents a close call. Their claim that time spent mitigating the effects of the breach constitutes a concrete injury has support in pre-*TransUnion* caselaw in this circuit. In both *Remijas* and *Lewert*, the Seventh Circuit concluded that time and money spent by plaintiffs "protecting themselves against future identity theft and fraudulent charges" in the wake of data breaches that compromised their credit card information constituted an injury in fact. *Remijas*, 794 F.3d at 694; *Lewert*, 819 F.3d at 966–67. And in *Craftwood II, Inc. v. Generac Power Systems, Inc.*, the Seventh Circuit held that even an "identifiable trifle" such as the time spent reading unlawfully sent incoming faxes is a concrete injury. 920 F.3d 479, 481 (7th Cir. 2019) (quoting *United States v. SCRAP*, 412 U.S. 669, 689 & n.14 (1973)). OneTouchPoint argues that the Supreme Court's 2021 *TransUnion* decision marked a dramatic shift in standing law. (ECF No. 55-1 at 25 (quoting *Dinerstein v. Google, LLC*, 73 F.4th 502, 516 (7th Cir. 2023).) It points to courts throughout the country that have rejected lost time as an injury for standing purposes, "finding it is not a legally cognizable concrete injury." (*Id.* at 27.) OneTouchPoint also cites the Supreme Court's decision in *Clapper v. Amnesty International USA*, in which the Court emphasized that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves

based on their fears of hypothetical future harm that is not certainly impending." 568 U.S. 398, 416 (2013).[2] But as *Remijas* makes clear, *Clapper* did not foreclose the possibility that mitigation efforts might constitute injuries sufficient to support standing. "*Clapper* was addressing speculative harm based on something that may not even have happened to some or all of the plaintiffs," in contrast to a data breach, where there is no dispute that the initial breach has occurred. *Remijas*, 794 F.3d at 694. Under *Remijas*, Plaintiffs' mitigation efforts may support standing if they plausibly allege that they undertook those efforts in the face of an imminent or "certainly impending" risk of harm as a result of the breach. *Id.* at 692 (citing *Clapper*, 568 U.S. at 416). Plaintiffs have at least alleged such conduct here and this Court remains bound by *Remijas*. Accordingly, Plaintiffs' alleged mitigation efforts taken in the face of impending harm remain sufficient under Seventh Circuit law.

OneTouchPoint attempts to distinguish *Remijas* and *Lewert* by arguing that the credit card data stolen in those cases created a more substantial risk of harm and that, unlike in those cases, Plaintiffs have not alleged "confirmed exfiltration" of their data. (ECF No. 62 at 10.) Both arguments are misplaced. For starters, Plaintiffs do allege that their data was exfiltrated. (ECF No. 15 ¶¶14–15.) And they spend a considerable portion of the Consolidated Complaint detailing the alleged harms that stem from data breaches, specifically from the theft of both SSNs and medical information. (*Id.* ¶¶110–60.) Moreover, as in *Remijas* and *Lewert*, several of the plaintiffs in this case allege actual identity theft and fraud as a result of the breach, (*see id.* ¶¶224, 234, 264, 284), and the rest allege that they face a "present and imminent threa[t] of fraud and identity theft" as a result of the breach at issue. (*Id.* ¶13.) While the latter allegation might, on its own, be too conclusory to support standing, it is bolstered by Plaintiffs' additional allegations, including assertions about warnings from the FBI, Secret Service, and Federal Trade Commission (FTC) concerning the dangers of cyberattacks and identity theft. While Plaintiffs do not allege that Guertin, Meza, Nardi, and Young have experienced actual identity theft or fraud, they allege that each has spent time and effort combatting the impending effects of the breach. *See Lewert*, 819 F.3d at 967 (holding that "time and effort" spent monitoring financial information "as a guard

[2] *Clapper* framed the standing analysis of mitigation costs in traceability terms, standing's second element. *See Clapper*, 568 U.S. at 416 ("Any ongoing injuries that respondents are suffering are not fairly traceable to § 1881a.") Following *Clapper*, the Seventh Circuit has framed mitigation injuries in the data breach context in terms of standing's requirement that a plaintiff suffer an "actual" injury. *Remijas*, 794 F.3d at 694 ("Mitigation expenses do not qualify as actual injuries where the harm is not imminent.") Whether framed as an issue of injury-in-fact or traceability, the inquiry remains the same.

against fraudulent charges and identity theft" was a concrete injury for standing purposes). Guertin has spent time "carefully reviewing her accounts for fraudulent activity." (*Id.* ¶254.) Meza has "spent approximately 2–3 hours changing his passwords, updating his credit cards, and otherwise trying to protect himself against fraudulent activity as a result of the Data Breach." (*Id.* ¶214.) Nardi has "spent approximately 1.5 hours . . . freezing her credit score." (*Id.* ¶274.) And Young has spent time "reviewing his credit card bills and credit reports to monitor for fraudulent activity." (*Id.* ¶295.)

Plaintiffs may ultimately have trouble proving a causal connection between this alleged harm and the breach, but the Consolidated Complaint sufficiently alleges that most of the challenged Plaintiffs—specifically Guertin, Meza, Nardi, and Young—undertook mitigation efforts to combat a harm that was imminent or certainly impending. The majority of district courts in this circuit have concluded similarly in data breach cases, even in the wake of *TransUnion*. *See In re Mondelez Data Breach Litig.*, No. 23 C 3999, 2024 WL 2817489, at *3 (N.D. Ill. 2024) (collecting cases).

The Court agrees with OneTouchPoint, however with respect to the allegations relating to Plaintiff Dusterhoft. While the Consolidated Complaint alleges in detail the time the other Plaintiffs have spent mitigating the effects of the breach, there are no such allegations as to Dusterhoft. The Consolidated Complaint alleges only that he "anticipates spending considerable time and money . . . to mitigate and address harms caused by the Data Breach." (ECF No. 15 ¶247.) As explained above, a future injury is insufficient to establish standing in a suit for damages. Accordingly, Dusterhoft has not alleged an injury in fact and lacks standing to bring his claims for damages.[3]

B. Plaintiffs Lack Standing to Pursue Both Declaratory and Injunctive Relief.

OneTouchPoint also argues that Plaintiffs lack standing for their claims for declaratory or injunctive relief. (ECF No. 55-1 at 31–32.) In the Consolidated Complaint, Plaintiffs ask the Court to declare that OneTouchPoint violated a duty to protect Plaintiffs' data and that its data

[3] OneTouchPoint does not otherwise challenge Plaintiffs' standing to pursue their claims for damages, but, consistent with the Court's independent duty to ensure that its jurisdiction is secure, s*ee FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 378–79 (2024), the Court confirms that it has standing over the remaining plaintiffs' claims. Plaintiffs allege that Crosby, Meeks, Haid, and Strickland have each experienced some form of actual identity theft or financial fraud following the breach. (ECF No. 15 ¶¶224, 234, 264, 284.) These allegations establish injury-in-fact. *See Remijas*, 794 F.3d at 692. *Remijas* also confirms that Plaintiffs' alleged injuries are fairly traceable to the breach and can be remedied by the recovery of damages. *See id.*

security practices violate federal and state law. They also ask the Court to enjoin OneTouchPoint from continuing those unlawful practices and affirmatively require it to institute various training and data security measures. (ECF No. 15 ¶¶544–45.) OneTouchPoint contends these requests fail because the proposed relief would not stop future misuse of Plaintiffs' data by those who accessed it in the data breach and because the Consolidated Complaint does not allege that a future incident is likely. (ECF No. 55-1 at 31–32.)

Plaintiffs' allegations of future injury are too conjectural to support standing for injunctive relief. "Unlike with damages, a past injury alone is insufficient to establish standing for purposes of prospective injunctive relief." *Simic v. City of Chicago*, 851 F.3d 734, 738 (7th Cir. 2017). To have standing for injunctive relief, a plaintiff must plausibly allege "a 'real and immediate' threat of future injury as opposed to a threat that is merely 'conjectural or hypothetical.'" *Id.* (quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983)). In stark contrast to their extensive allegations concerning the breach that occurred, spanning the bulk of their 136-page Consolidated Complaint, Plaintiffs provide only scant conclusory allegations concerning the risk that they will suffer harm from another data breach at OneTouchPoint. Their brief directs the Court to two paragraphs in the Consolidated Complaint, which allege only that Plaintiffs have a continuing interest in protecting their data in OneTouchPoint's possession and that OneTouchPoint's "data security measures remain inadequate," which puts them "at imminent risk that further compromises of their Private Information still in [OneTouchPoint's] possession . . . will occur in the future. (ECF No. 59 at 23; ECF No. 15 ¶¶202, 543.) Plaintiffs allege no specific facts establishing how OneTouchPoint's data security remains inadequate, or how they face a real and immediate threat of future injury from another data breach occurring due to OneTouchPoint's failure to protect their data. And while Plaintiffs may face a continuing threat of harm from the breach that has already occurred, an injunction requiring OneTouchPoint to change their data security practices will not redress those injuries. Accordingly, Plaintiffs' claims for injunctive relief will be dismissed for lack of standing.

Plaintiffs also lack standing to pursue their claims for declaratory relief. Pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201, they seek declarations that OneTouchPoint owes them a duty to protect their data, that it breached that duty, that its "acts and omissions" as alleged in the Consolidated Complaint violate state law, and that its data security practices are unlawful. (ECF No. 15 ¶544.) A request for declaratory judgment does not require the same threat of future

harm as one for injunctive relief, but a plaintiff must still satisfy standing's requirements of injury-in-fact, traceability, and redressability. *See Stencil v. Johnson*, 605 F. Supp. 3d 1109, 114 (E.D. Wis. 2022); *see also TransUnion*, 594 U.S. at 431 (noting that a plaintiff must establish standing for each form of relief sought). Here, the issue is one of redressability. As discussed above, Plaintiffs have alleged injuries sufficient to support standing stemming only from a data breach that has already occurred. And like their requests for injunctive relief, Plaintiffs' requested declaratory relief would do nothing to redress those injuries. Declarations that OneTouchPoint breached a duty it owed them or otherwise acted unlawfully would not, standing alone, provide any relief to Plaintiffs. Moreover, "[d]eclaratory relief 'presupposes the existence of a judicially remediable right' and thus cannot be pursued without a predicate right of action." *Alarm Detection Sys., Inc. v. Orland Fire Prot. Dist.*, 929 F.3d 865, 871 n.2 (7th Cir. 2019) (quoting *Schilling v. Rogers*, 363 U.S. 666, 677 (1960)). Where Plaintiffs have adequately alleged that OneTouchPoint breached an actionable duty, they have standing to pursue claims for damages. Their requested declaratory relief, divorced from any independent right of action, is improper.[4]

II. OneTouchPoint's Motion to Dismiss Under Rule 12(b)(6) Will Be Granted in Part and Denied in Part.

OneTouchPoint also seeks dismissal of Plaintiffs' claims on grounds that the allegations in the Consolidated Complaint are insufficient to state a claim under the substantive legal theories they invoke. Plaintiffs assert nineteen substantive claims, based on both common-law and statutory theories, but have withdrawn two of those claims during the briefing (a common-law claim for breach of implied contract and a statutory claim under Wisconsin's Right to Privacy Act). (*See* ECF No. 59 at 35 n.17, 35.) Plaintiffs also concede that they seek only injunctive relief on two other claims, under Maine's and Georgia's Uniform Deceptive Trade Practices Acts, (*see id.* at 43, 48), and, given Plaintiffs' lack standing to pursue injunctive relief, those claims must also be dismissed. Finally, the Court will not address Plaintiffs' statutory claims on behalf of Plaintiff Dusterhoft under Minnesota's Consumer Fraud, Uniform Deceptive Trade Practices, and Health

[4] To the extent Plaintiffs have standing to support a request for declaratory relief, the Court would exercise its discretion not to declare the parties' rights. *See* 28 U.S.C. § 2201(a) ("[A]ny court of the United States . . . *may* declare the rights and other legal relations of any interested party seeking such declaration.") (emphasis added); *see also Wilton v. Seven Falls Co.*, 515 U.S. 277, 282 (1995) ("[D]istrict courts possess discretion in determining whether and when to entertain an action under the Declaratory Judgment Act, even when the suit otherwise satisfies subject matter jurisdictional prerequisites."). Because Plaintiffs' requests for declaratory relief are duplicative of their claims for damages, the Court concludes there is no cause to entertain those requests, even if Plaintiffs have standing.

Records Acts, (ECF No. 15 ¶¶492–532), given Dusterhoft's lack of standing. The Court will address OneTouchPoint's arguments on the balance of Plaintiffs' claims, starting with Plaintiffs' common-law causes of action.

A. Plaintiffs State Common-Law Claims for Negligence, Negligence Per Se, and Unjust Enrichment.

Plaintiffs assert common-law claims for negligence, negligence per se, breach of fiduciary duty, breach of third-party beneficiary contract, and unjust enrichment. In evaluating whether Plaintiffs' allegations are sufficient to support these claims, the Court must first tackle a potentially thorny choice-of-law issue. Federal courts sitting in diversity apply the choice-of-law rules of the forum state. *See Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 792–93 (W.D. Wis. 2019) (citing *Auto-Owners Ins. Co. v. Websolv Computing, Inc.*, 580 F.3d 543, 547 (7th Cir. 2009)). Under Wisconsin choice-of-law rules, decisions regarding choice-of-law "are made on an issue-by-issue basis." *Id.* at 793 (citing *BB Syndication Servs., Inc. v. First Am. Title Ins. Co.*, 780 F.3d 825, 829 (7th Cir. 2015)). The Seventh Circuit has wisely suggested, however, that "before entangling itself in messy issues of conflict of laws a court ought to satisfy itself that there actually is a difference between the relevant laws of the different states." *Jean v. Dugan*, 20 F.3d 255, 260 (7th Cir. 1994) (quoting *Barron v. Ford Motor Co. of Canada, Ltd.*, 965 F.2d 195, 197 (7th Cir. 1992)). And if there is no disagreement among the states, the law of the forum state applies. *Id.* (citing *Int'l Admins. v. Life Ins. Co.*, 753 F.2d 1373, 1376 n.4 (7th Cir. 1985)).

Wisconsin's choice-of-law rules begin with the premise that "the law of the forum should presumptively apply unless it becomes clear that nonforum contacts are of the greater significance." *State Farm Mut. Auto. Ins. Co. v. Gillette*, 641 N.W.2d 662, 676 (Wis. 2002) (quoting *Hunker v. Royal Indem. Co.*, 204 N.W.2d 897, 902 (Wis. 1973)). If it is not clear that the nonforum contacts are of greater significance, a five-factor test applies: (1) predictability of results; (2) maintenance of interstate and international order; (3) simplification of the judicial task; (4) advancement of the forum's governmental interests; and (5) application of the better rule of law. *Id.* at 676.

OneTouchPoint argues that "the law of the state where reach Plaintiff resides should apply, as it is the location of their alleged harm." (ECF No. 55-1 at 34.) It also argues that Wisconsin's factor test weighs in favor of applying the law of the state where each Plaintiff resides. (*Id.*) Plaintiffs counter that a choice-of-law analysis is premature. (ECF No. 59 at 23.) They argue that "discovery will reveal where the breached data was maintained and where [OneTouchPoint's]

security protocols failed." (*Id.*) They ask the Court to apply Wisconsin law in ruling on the motion to dismiss, insisting that, even if a choice-of-law analysis was appropriate at this phase of litigation, OneTouchPoint has not identified meaningful distinctions in the laws of the relevant states. (*Id.* at 24.) The eight remaining plaintiffs reside in Wisconsin (Haid, Nardi, and Crosby), Arizona (Meza), Georgia (Meeks and Strickland), Maine (Young), and South Carolina (Guertin).

With respect to Haid, Nardi, and Crosby, Wisconsin law plainly applies. Each is a Wisconsin resident, so any harm to them presumptively happened in Wisconsin. And while the Consolidated Complaint does not allege where the data breach occurred, OneTouchPoint is headquartered in Wisconsin and there are no allegations that implicate any other state. For the remaining named Plaintiffs, the choice-of-law analysis is more complicated. The other Plaintiffs have minimal contacts to Wisconsin or to this forum. The Consolidated Complaint alleges only that Plaintiffs' information was subject to a data breach at OneTouchPoint, which is headquartered in this state and "conducts substantial business" here. (*See* ECF No. 15 ¶¶33, 35.) As Plaintiffs point out, discovery will provide necessary information about where the breach and OneTouchPoint's allegedly unlawful behavior occurred. Because the Defendant is nonetheless headquartered in Wisconsin, it seems reasonably likely that the breach occurred in Wisconsin, providing significant ties between the forum state and all other Plaintiffs' claims. On the current record at least, the Court cannot conclude that any other state has more significant contacts to the claims of any of the Plaintiffs.

Moreover, as noted repeatedly below, the parties have identified few meaningful differences between Wisconsin law and the laws of the other states potentially at issue. Accordingly, for most of Plaintiffs' common-law claims the Court may apply Wisconsin law without reservation. *See Dugan*, 20 F.3d at 260. In those few instances where the parties have identified meaningful distinctions, the Court still finds it appropriate to apply Wisconsin law at this early pleading stage in the litigation. As discussed above, Wisconsin's contacts to this case, as it pertains to Plaintiffs who reside in other states, are uncertain based on the Consolidated Complaint. The Court cannot reasonably conclude that "nonforum contacts are of the greater significance" as to any Plaintiff. *See Gillette*, 641 N.W.2d at 676 (quoting *Hunker*, 204 N.W.2d at 902). And application of Wisconsin's five-factor test is unlikely to provide further clarity at this early stage, given the uncertainty of the forum state's connection to the data breach. Given the minimal material disagreements between the parties, the Court concludes that it is most appropriate

to apply Wisconsin law to all Plaintiffs' common-law claims at the pleading stage and decide choice-of-law issues as the litigation progresses. *See Mirfasihi v. Fleet Mortg. Corp.*, 450 F.3d 745, 750 (7th Cir. 2006) ("[T]he choice-of-law issues in nationwide class actions are rarely so uncomplicated that one can delineate clear winning and losing arguments at an early stage in the litigation.").

1. Plaintiffs Have Pleaded a Claim for Negligence.

Plaintiffs allege that OneTouchPoint was negligent in failing to protect their data from the breach. (ECF No. 15 ¶¶310–20.) In Wisconsin, a negligence claim has four elements: (1) a duty of care owed by the defendant; (2) breach of that duty; (3) a causal connection between the breach and the plaintiff's injury; and (4) actual loss or damage resulting from the injury. *Hornback v. Archdiocese of Milwaukee*, 752 N.W.2d 862, 867 (Wis. 2008) (citing *Gritzner v. Michael R.*, 611 N.W.2d 906, 912 (Wis. 2000)). The elements are the same in the other relevant states. (*See* ECF No. 55-1 at 35 n.3 (collecting cases).) OneTouchPoint challenges the sufficiency of Plaintiffs' pleading on the last two elements, arguing that Plaintiffs only speculatively allege causation and fail to plead compensable damages. (ECF No. 55-1 at 35–39.)

OneTouchPoint's first argument is that Plaintiffs' allegations of causation are purely speculative. (ECF No. 55-1 at 35–36 (citing *Shanley v. Omega Flex, Inc.*, No. 19-cv-664-slc, 2021WL 778921, at *3 (W.D. Wis. Mar. 1, 2021); *Spivey-Johnson v. SM&P Util. Res., Inc.*, No. 05-C-0087, 2007 WL 81883, at *3 (E.D. Wis. Jan. 8, 2007).) At the pleading stage, Plaintiffs are only required to allege facts raising a plausible inference that OneTouchPoint's negligence caused their injuries, but OneTouchPoint insists that the Consolidated Complaint "makes no allegations plausibly connecting" Plaintiffs' injuries to the data breach. (*Id.* at 36.) More specifically, OneTouchPoint argues that "only Plaintiffs Crosby, Haid, Meeks, and Strickland are alleged to have experienced actual misuse of their" data and that, among those plaintiffs, only Crosby and Haid allege that their SSNs were compromised. (*See id.*) It further argues that the Consolidated Complaint focuses only on the potential danger when one's SSN is compromised and, therefore, the Plaintiffs who only had their names, addresses, dates of birth, and some health information compromised have not plausibly alleged that any injury they suffered was caused by the data breach. (*Id.* at 36–37.)

OneTouchPoint's argument may have merit, but it is better suited for summary judgment. While the Consolidated Complaint focuses on the harms caused by theft of SSNs, it also alleges

that private health information and private information in general can and do lead to identity theft. (*See* ECF No. 15 ¶¶118, 120, 126, 132–34, 150–53.) Plaintiffs also allege that OneTouchPoint informed each of them that, at the very least, personally identifying information and private health information was compromised in the breach. (*See id.* ¶¶220, 230, 250, 270, 290.) And they allege that their injuries were a result of the breach, whether actual identity theft or mitigation injuries. (*See id.* ¶¶197–98, 214, 224, 234, 254, 264, 274, 284, 295.) Additionally, Plaintiffs allege that OneTouchPoint sent them letters encouraging them "to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring free credit reports for suspicious activity, and to detect errors." (*Id.* ¶¶168, 210, 220, 240, 250, 260, 270, 280.) Plaintiffs may ultimately be unable to prove that their injuries were caused by the data breach, but their allegations are sufficient at the pleading stage. *See Iqbal*, 556 U.S. at 678.

OneTouchPoint's arguments as to damages are also procedurally misplaced. OneTouchPoint argues that Plaintiffs have pleaded damages that are unavailable in a negligence action under various state laws, or too speculative to support a claim for negligence. (ECF No. 55-1 at 37–39.) While these arguments may have merit under state law, they are not appropriate for a motion to dismiss in federal court. "[I]n federal court it is the federal rules that determine what must be in a complaint." *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018). And Rule 8 "does not require detail about the nature of the plaintiff's injury. *Id.* (citing *Lujan*, 504 U.S. at 561). At the pleading stage, a plaintiff who has alleged an injury-in-fact sufficient to support standing has suffered damages. *Id.* Accordingly, Plaintiffs have adequately pleaded their negligence claims.

2. Plaintiffs Sufficiently Allege Claims for Negligence Per Se.

Plaintiffs allege that OneTouchPoint was per se negligent based on violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules and Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1).[5] (ECF No. 15 ¶¶321–32.) Wisconsin recognizes a separate cause of action for negligence per se when the defendant's breach of duty stems from a violation of a "safety statute." *See Cooper v. Eagle River Mem'l Hosp., Inc.*, 270 F.3d 456, 460 (7th Cir. 2001). A negligence per se claim requires that: "(1) the harm inflicted was the type the statute was

[5] Plaintiffs also invoke the Wisconsin Constitution and Wisconsin Right to Privacy Act, Wis. Stat. § 995.50(2), (ECF No. 15 ¶326), but fail to allege how OneTouchPoint violated duties created by either and appear to have abandoned both as sources for duties OneTouchPoint breached.

designed to prevent; (2) the person injured was within the class of persons sought to be protected; and (3) there is some expression of legislative intent that the statute become a basis for the imposition of civil liability." *Id.* (quoting *Antwaun A. v. Heritage Mut. Ins. Co.*, 596 N.W.2d 456, 466 (Wis. 1999)). Georgia and South Carolina have similar standards. *See Goldstein, Garber & Salama, LLC v. J.B.*, 797 S.E.2d 87, 92 (Ga. 2017); *Whitlaw v. Kroger Co.*, 410 S.E.2d 251, 252 (S.C. 1991). HIPAA's Privacy and Security Rules establish national standards for protecting individuals' private health information. *See* 45 C.F.R. pts. 160 & 164 subpts. A, C, E. Section 5 of the FTC Act prohibits "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce . . . ." 15 U.S.C. § 45(a)(1).

OneTouchPoint first argues for dismissal on grounds that Plaintiffs Meza and Young cannot maintain negligence per se claims because their home states, Arizona and Maine, do not recognize a separate cause of action for negligence per se. (ECF No. 55-1 at 39 n.5 (collecting cases).) Plaintiffs concede that Maine does not recognize negligence per se and agree to drop Young's claim under Maine law. (ECF No. 59 at 31 n.12.) But Plaintiffs dispute OneTouchPoint's contention concerning Meza, pointing to *Lewis v. Dirt Sports LLC*, 259 F. Supp. 3d 1039, 1045 (D. Ariz. 2017), which they contend acknowledges that Arizona recognizes a cause of action for negligence per se. (ECF No. 59 at 31 n.12.) Plaintiffs appear to be correct. *Lewis* confirms that (whether considered a "separate" cause of action or simply another theory of negligence) Arizona law recognizes claims for negligence per se. *See Lewis*, 259 F. Supp. 3d at 1045 (citing *Good v. City of Glendale*, 722 P.2d 386, 389 (Ariz. Ct. App. 1986)). But because the Court is preliminarily examining Plaintiffs' common-law claims under Wisconsin law, these distinctions are, at present, superfluous.

OneTouchPoint also argues that Plaintiffs' negligence per se claims should be dismissed because they have only alleged in conclusory fashion that they are within the class of persons sought to be protected by HIPAA and Section 5 of the FTC Act, and because neither statute includes an expression of legislative intent for the statute to serve as the basis for civil liability. (ECF No. 55-1 at 40.) In response, Plaintiffs point to paragraphs in the Consolidated Complaint detailing the HIPAA rules and FTC Act and alleging that Plaintiffs are among the class of persons those laws seek to protect. (ECF No. 59 at 32 (citing ECF No. 15 ¶¶44–51, 84–94, 329–30).) Plaintiffs also cite caselaw from courts applying Wisconsin law and other jurisdictions upholding claims for negligence per se based on alleged violations of Section 5 of the FTC Act. (*Id.* at 32–

33.) OneTouchPoint is correct that Plaintiffs' allegation that they "are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTC Act . . . was intended to protect," (*see* ECF No. 15 ¶329), is conclusory. But those are not Plaintiffs' only allegations concerning HIPAA and the FTCA. The Consolidated Complaint also alleges that "[t]he HIPPA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity." (ECF No. 15 ¶45 n.3.) And it alleges that the FTC "has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an 'unfair practice' in violation of the [FTCA]." (*Id.* ¶84.) These allegations support a reasonable inference that the HIPAA rules seek to protect healthcare patients' records and Rule 5 of the FTCA seeks to protect consumers' personal data. Thus, Plaintiffs have sufficiently alleged they are within the class of persons both laws seek to protect.

OneTouchPoint next seeks dismissal on grounds that "[n]either HIPAA nor the FTC Act explicitly authorize a private cause of action, and there is no legislative authority that Congress intended them to protect individuals affected by data breaches." (ECF No. 55-1 at 40 (collecting cases confirming HIPAA and FTC Act do not have a private right of action).) While OneTouchPoint is correct that neither HIPAA nor Section 5 creates a private right of action, that is not necessarily required for a claim of negligence per se. Negligence per se claims require evidence of legislative intent that the statute become a basis for the imposition of civil liability. *Cooper*, 270 F.3d at 460. Both HIPAA and Section 5 authorize the federal government to impose civil liability for violations akin to those OneTouchPoint is accused of committing. *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015); *see also* 45 C.F.R. § 160.402. OneTouchPoint cites several cases from other districts dismissing similar claims, (ECF No. 55-1 at 40–41 (citing *In re: Netgain Tech.,* LLC, No. 21-cv-1210, 2022 WL 1810606, at *16 (D. Minn. June 2, 2022); *J.R. v. Walgreens Boots All., Inc.*, 470 F. Supp. 3d 534, 553–54 (D.S.C. 2020)), but only *Netgain* applies Wisconsin law. And the *Netgain* court dismissed the claim based on the lack of an express private right of action in the FTC Act. *See Netgain*, 2022 WL 1810606, at *16. In response, Plaintiffs cite cases from several jurisdictions upholding negligence per se claims based on a violation of Section 5 of the FTC. (*See* ECF No. 59 at 32 (collecting cases).) Neither party cites to any relevant authority from the Seventh Circuit or Wisconsin courts.

Ultimately, the parties' briefing on this issue is lacking. At this stage, the Court concludes that Plaintiffs have alleged sufficient facts for their negligence per se claims to survive this motion to dismiss. But the Court is not convinced that either HIPAA or the FTC Act can form the basis for negligence per se, and OneTouchPoint can renew this argument at summary judgment. Accordingly, for now, Plaintiffs' negligence per se claims may proceed.

3. Plaintiffs' Fiduciary Duty Claim Fails Because They Have Not Plausibly Alleged a Fiduciary Relationship with OneTouchPoint.

Plaintiffs allege that, as a "business associate" of Plaintiffs' healthcare providers, OneTouchPoint had a fiduciary duty to act for the benefit of Plaintiffs and safeguard their private information. (ECF No. 15 ¶335.) In Wisconsin, a breach of fiduciary duty claim requires: (1) the existence of a fiduciary duty from the defendant to the plaintiff; (2) breach of that duty; and (3) damages caused by the breach. *Berner Cheese Corp. v. Krug*, 752 N.W.2d 800, 809 (Wis. 2008). The elements appear to be the same in the other relevant states. (ECF No. 55-1 at 41 n.7 (collecting cases).)

OneTouchPoint asserts that Plaintiffs' breach of fiduciary claim must be dismissed because, as a matter of law, OneTouchPoint had no fiduciary relationship with Plaintiffs and, thus, owed them no fiduciary duty. (ECF No. 55-1 at 42–43). "A fiduciary relationship arises from a formal commitment to act for the benefit of another . . . or from special circumstances from which the law will assume an obligation to act for another's benefit." *Doe v. Archdiocese of Milwaukee*, 700 N.W.2d 180, 194 (Wis. 2005) (quoting *Merrill Lynch v. Boeck*, 377 N.W.2d 605, 609 (Wis. 1985)). Fiduciary duties are "those obligations that are peculiar to a fiduciary and are based on the conscious undertaking of a special position with regard to another." *Zastrow v. J. Commc'ns, Inc.*, 718 N.W.2d 51, 59 (Wis. 2006).

As for the majority of Plaintiffs, whose data was provided to OneTouchPoint by Plaintiffs' medical providers or insurers, OneTouchPoint argues that its relationship with those Plaintiffs is too indirect and attenuated to support the imposition of a fiduciary duty. (*See* ECF No. 55-1 at 42–43). It notes that the Consolidated Complaint alleges that Plaintiffs Guertin, Meeks, Haid, Nardi, Young, and Strickland provided their information to OneTouchPoint's customers, not to OneTouchPoint itself. (*See id.* at 42.) And there is no allegation that Plaintiffs "had any communication with, relationship to, or even knowledge of OneTouchPoint . . . prior to receiving notice of the [data breach]" (*Id.*) Nor is there any alleged formal legal relationship between the

parties, or other basis to impose on OneTouchPoint a duty to act for Plaintiffs' benefit, or any plausible suggestion that Plaintiffs placed any trust or confidence in OneTouchPoint that it abused. (*Id.* at 42–43.)

Plaintiffs respond by arguing that "a fiduciary relationship was found in almost an identical circumstance as to that here," citing *Purvis v. Aveanna Healthcare, LLC*, 563 F. Supp. 3d 1360 (N.D. Ga. 2021). (ECF No. 59 at 33.) And they direct the Court to allegations in the complaint that "[OneTouchPoint] requires patients to provide personal information to its healthcare customers before it provides them services" and to OneTouchPoint's privacy policy from its website. (ECF No. 59 at 34 (citing ECF No. 15 ¶¶39, 41).) Plaintiffs' heavy reliance on *Purvis* is misplaced. Contrary to Plaintiffs' suggestion, *Purvis* did not involve an "almost an identical circumstance." *Purvis* involved a data breach at a healthcare provider to whom plaintiffs had *directly* given their personal and health information. *See* 563 F. Supp. 3d at 1383. In this setting, the court concluded that the direct relationship between the parties, in which "the patient-Plaintiffs shar[ed] and disclos[ed] private health information with Defendant that was akin to the health information that would be communicated to a physician when receiving medical care," was sufficient, under Georgia law, to state a claim for breach of fiduciary duty. *Id.* There are no similar allegations here. Nor do Plaintiffs provide any other support for their assertion that, simply by contracting with Plaintiffs' healthcare insurers and providers, OneTouchPoint became a fiduciary with respect to Plaintiffs. The Consolidated Complaint alleges that "[a]s a regular part of its business, [OneTouchPoint] requires patients to provide personal information to its healthcare customers before it provides them services." (ECF No. 15 ¶39.) But this conclusory allegation is out of step with the balance of the Consolidated Complaint and there are no allegations that Plaintiffs and OneTouchPoint had any direct relationship.

Plaintiffs fare no better by directing the Court to their allegations concerning the Privacy Policy on OneTouchPoint's website. This policy allegedly provides that the company has "put in place appropriate procedures with the services providers we share your Personally Identifiable Information with to ensure that your Personally Identifiable Information is treated by those service providers in a way that is consistent with, and which respects the applicable laws on data security and privacy." (*Id.* ¶41.) Plaintiffs characterize these statements as "direct representations to Plaintiffs that they could repose their trust and Private Information" in OneTouchPoint. (ECF No. 59 at 34.) But this language does not suggest the existence of a fiduciary relationship. Fiduciary

relationships exist in many contexts: "trustee to beneficiary, guardian to ward, agent to principal, attorney to client." *Zastrow*, 718 N.W.2d at 59 (quoting Eileen A. Scallen, *Promises Broken v. Promises Betrayed: Metaphor, Analogy, and The New Fiduciary Principle*, 1993 U. Ill. L. Rev. 897, 905–06). Central to those relationships is a substantial degree of trust and authority exercised by the fiduciary over the affairs of the other party. Nothing in the privacy policy plausibly suggests such a relationship existed here. Accordingly, Plaintiffs' allegations do not state a claim for breach of fiduciary duty as to Plaintiffs Haid, Nardi, Meeks, Strickland, Young, and Guertin and the fiduciary duty claims as to those Plaintiffs must be dismissed.

The remaining Plaintiffs, Meza and Crosby, stand in a different relationship to OneTouchPoint. Both were OneTouchPoint employees who directly provided information to the company pursuant to their employment. Plaintiffs fail to allege (or even argue) that the employment relationship between OneTouchPoint on the one hand and Meza and Crosby on the other gave rise to fiduciary duties related to their information. Having offered no allegations supporting the existence of such a relationship and having offered no argument in response to OneTouchPoint's motion, Plaintiffs' breach of fiduciary duty claims with respect to these Plaintiffs will also be dismissed.

4. Plaintiffs' Third-Party Beneficiary Claims Fail Because They Have Not Plausibly Alleged That They Were Direct and Primary Beneficiaries of OneTouchPoint's Contracts with Their Healthcare Providers.

Plaintiffs allege that OneTouchPoint contracted with Plaintiffs' healthcare providers for the purpose of "providing care strategies, consulting, analytics, and other services," and "expressly for the benefit of Plaintiffs . . . ." (ECF No. 15 ¶¶341–43.) On this claim, the parties agree that Wisconsin law applies. (ECF No. 55-1 at 45 n.10; *see also* ECF No. 59 at 35 (applying only Wisconsin law).) Under Wisconsin law, a third-party beneficiary "must show that the contracting parties entered into the agreement for the direct and primary benefit of the third party, either specifically or as a member of a class intended to benefit from the contract." *Sussex Tool & Supply, Inc. v. Mainline Sewer & Water, Inc.*, 605 N.W.2d 620, 623 (Wis. Ct. App. 1999). "An indirect benefit incidental to the primary purpose of the contract is insufficient to confer third-party beneficiary status." *Id.*

OneTouchPoint argues that Plaintiffs' breach of third-party beneficiary contract claim fails because Plaintiffs provide only "contradictory and conclusory allegations regarding contracts between OneTouchPoint and its customers." (ECF No. 55-1 at 46.) Plaintiffs allege that

OneTouchPoint "is a mailing and printing services vendor, which offers print, marketing execution, and supply chain management services to organizations in the healthcare sector." (ECF No. 15 ¶2.) Yet, in alleging breach of a third-party beneficiary contract, Plaintiffs allege that OneTouchPoint entered into contracts with its clients to provide "care strategies, consulting, analytics, and other services," and then (apparently mistakenly) refer to OneTouchPoint as "MCG Health." (*See id.* ¶341.) Plaintiffs make no attempt to clarify these confusing allegations in their briefing. Instead, Plaintiffs argue that OneTouchPoint "acquired their Private Information from healthcare organizations and touted its ability to keep that data confidential." (ECF No. 59 at 35.) Plaintiffs further argue that the healthcare organizations who provided their data to OneTouchPoint have a statutory obligation to protect Plaintiffs' information and that OneTouchPoint "accepted the Private Information of Plaintiffs from healthcare providers on the condition that it employ reasonable safeguards to protect the Private Information that [OneTouchPoint] was entrusted with." (*Id.*)

None of Plaintiffs' allegations plausibly support an inference that Plaintiffs were intended to be the "direct and primary" beneficiaries of OneTouchPoint's contracts with Plaintiffs' healthcare providers. *See Sussex Tool*, 605 N.W.2d at 623. At most, Plaintiffs have alleged that protection of their private data was a benefit incidental to the primary purpose of those contracts. Because this is insufficient to sustain a claim, Plaintiffs' third-party beneficiary claims will be dismissed.

5. Plaintiffs, Except Meza and Crosby, Have Stated a Claim for Unjust Enrichment.

In support of their unjust enrichment claim, Plaintiffs allege that they "conferred a monetary benefit upon [OneTouchPoint] in the form of monies paid for healthcare services or other services" and it would be "inequitable and unjust" for OneTouchPoint to retain that benefit following the data breach. (ECF No. 15 ¶¶363, 371.) Under Wisconsin law, an unjust enrichment claim requires proof of: "(1) a benefit conferred upon the defendant by the plaintiff; (2) an appreciation or knowledge by the defendant of the benefit; and (3) acceptance or retention by the defendant of the benefit under circumstances making it inequitable for the defendant to retain the benefit without payment of its value." *Puttkammer v. Minth*, 266 N.W.2d 361, 363 (Wis. 1978) (collecting cases). The standards are similar in the other relevant states. (ECF No. 55-1 at 49 n.13 (collecting cases).)

OneTouchPoint argues that Plaintiffs have not alleged that they paid OneTouchPoint for services, and any money paid to OneTouchPoint's customers that was in turn paid to OneTouchPoint "is far too attenuated and speculative to form the basis for an unjust enrichment claim." (ECF No. 55-1 at 49–50.) It further contends that the relevant states do not permit unjust enrichment claims based on an indirect benefit and that similar claims have failed in other data breach cases. (*Id.* at 50–51.) Plaintiffs respond that the relevant states allow unjust enrichment claims based on an indirect benefit, like that alleged here, and, regardless, the benefit they conferred on OneTouchPoint was a direct benefit that simply "flow[ed] through a third party." (ECF No. 59 at 36–37.) OneTouchPoint's arguments for dismissal largely miss the mark. As Plaintiffs point out, this Court has previously concluded that Wisconsin law does not preclude recovery for unjust enrichment when only an indirect benefit was conferred on the defendant. *See BMO Harris Bank v. Berkovitz*, No. 20-C-546, 2020 WL 5877682, at *3 (E.D. Wis. Oct. 2, 2020).

OneTouchPoint also contends that Plaintiffs' unjust enrichment claims are doomed by the Consolidate Complaint's failure to plausibly allege that Plaintiffs had any knowledge or expectation of OneTouchPoint protecting their data, since they are not alleged to have even known of its existence prior to the data breach. (ECF No. 62 at 19.) In response, Plaintiffs point to allegations that they provided their private information to OneTouchPoint in exchange for health services, which they would not have done had they known OneTouchPoint would not protect that information. (*See* ECF No. 59 at 37 (citing ECF No. 15 ¶¶45, 51, 188, 363–64).) They claim these allegations are sufficient to state unjust enrichment claims. OneTouchPoint's focus on Plaintiffs' lack of knowledge misstates the second element of an unjust enrichment claim. The issue is not Plaintiff's knowledge, but whether OneTouchPoint—as the defendant—had knowledge of the benefit conferred upon it. This element Plaintiffs have alleged.

In the end, the Court is again sympathetic to OneTouchPoint's argument that Plaintiffs' allegation that money they paid to OneTouchPoint's customers was then paid to them "is far too attenuated and speculative to form the basis for an unjust enrichment claim." (ECF No. 55-1 at 49–50.) But OneTouchPoint has not cited Wisconsin caselaw sufficient to support dismissal on this ground. While OneTouchPoint points to district court decisions in South Carolina and Florida dismissing unjust enrichment claims in data breach cases, (ECF No. 55-1 at 50–51), those cases are not binding here and are, at this point, unpersuasive. While the Court is once again skeptical

of Plaintiffs' ultimate ability to prove their claim, they have alleged enough to state a claim for unjust enrichment. OneTouchPoint is free to challenge this theory again on summary judgment.

The parties are silent on the unjust enrichment claims brought on behalf of Plaintiffs Meza and Crosby, both of whom provided their personal information to OneTouchPoint pursuant to their employment, not through OneTouchPoint's customers. The Consolidated Complaint does not offer any factual allegations to support their claims of unjust enrichment as to Meza's and Crosby's information. Nor do Plaintiffs offer any argument in support of this claim in their briefing. The Court will not do their work for them. Accordingly, the Court will grant OneTouchPoint's motion to dismiss as to the unjust enrichment claims of only Meza and Crosby.

B. Plaintiffs' Allegations Support Their Statutory Claims Under Wisconsin, Georgia, and South Carolina Law Only.

In addition to their common-law claims, Plaintiffs assert seven statutory claims against OneTouchPoint, invoking specific legislation enacted in Wisconsin, Maine, Arizona, Georgia, and South Carolina. For the below reasons, the Court concludes that all Plaintiffs except Meza and Crosby have stated a claim under Wisconsin law for negligent release of their health records. The Court also concludes that Plaintiff Meeks has stated claims under Georgia's Fair Business Practices Act and that Plaintiff Guertin has stated a claim under the South Carolina Data Breach Security Act. Plaintiffs' other statutory claims for damages are legally insufficient, however, and will be dismissed.

1. Plaintiffs Have Stated a Claim Under Wisconsin Law Only for Negligent Release of Their Health Records.

The Consolidated Complaint asserts claims on behalf of all Plaintiffs under Wisconsin's health care records law, Wis. Stat. § 146.81, *et seq.*, and the Wisconsin Deceptive Trade Practices Act, Wis. Stat. § 100.18. As explained below, Plaintiffs, other than Meza and Crosby, have adequately stated a claim for negligent release of their health records under Wis. Stat. §§ 146.82(1), 146.84(1)(bm), but have failed to state a claim under the Wisconsin Deceptive Trade Practices Act. Accordingly, the latter claim will be dismissed.

a. Plaintiffs, Except Meza and Crosby, Have Stated Claims for Negligent Release of Their Health Records Under Wis. Stat. §§ 146.82(1), 146.84(1)(bm).

Plaintiffs claim that OneTouchPoint violated Wisconsin's health care records law by both negligently and "knowingly and willfully" failing to maintain adequate data security measures and thereby disclosing Plaintiffs' health care records to cybercriminals through the data breach. (ECF

No. 15 ¶¶375–82, 385.). Wis. Stat. § 146.82(1) reads, in relevant part: "Patient health records may be released only to the persons designated in this section or to other persons with the informed consent of the patient." Wis. Stat. § 146.84(1)(b) creates a private right of action for patients against anyone who knowingly and willfully negligently violates Section 146.82 and Section 146.84(1)(bm) against anyone who negligently violates the statute.

OneTouchPoint argues that the Consolidated Complaint fails to state a claim because it does not allege that OneTouchPoint "disclosed" Plaintiffs' health records to anyone; rather the health records were seized in a data breach that "was the result of unauthorized activity by a third party, of which OneTouchPoint had no knowledge or involvement." (ECF No. 55-1 at 51.) OneTouchPoint similarly contends that it did not "allow access" to Plaintiffs' health records within the meaning of the statute, which governs requests for access to records, not data breaches by hackers. (*Id.* at 51–52.)

Contrary to OneTouchPoint's contentions, Plaintiffs have sufficiently alleged claims under Section 146.84(1)(bm) for violation of Wis. Stat. § 146.82(1). While their allegation that OneTouchPoint "disclosed" their health records is poorly phrased, read as a whole the Consolidated Complaint alleges a violation of the statute. The appropriate inquiry is whether OneTouchPoint "released" Plaintiffs' records without their consent. Plaintiffs allege that OneTouchPoint both willfully and negligently released their records, (ECF No. 15 ¶381–82, 385), but appear to have abandoned the claim of willfulness in their briefing. (*See* ECF No. 59 at 37–38.) While OneTouchPoint argues that the statute requires an affirmative release of records, rather than negligently causing the release of records, it offers no support for this interpretation. (*See* ECF No. 62 at 20.) Wis. Stat. § 146.82(1) prohibits the unauthorized release of medical records and Wis. Stat. § 146.84(1)(bm) authorizes suit against anyone who negligently violates the statue. Plaintiffs allege that OneTouchPoint was negligent in allowing the data breach, which caused the release of their records. That satisfies the plain language of the statute and OneTouchPoint has provided no authority to the contrary. In *Fox v. Iowa Health Systems.*, the District Court for the Western District of Wisconsin concluded that similarly positioned plaintiffs stated a claim under the statute when their health records were compromised in a data breach. 399 F. Supp. 3d 780, 796 (W.D. Wis. 2019). The Court will follow *Fox* and, at least at the pleading stage, allow Plaintiffs to proceed with their Wis. Stat. § 146.84(1)(bm) claim for violation of Wis. Stat. § 146.82(1) based on the alleged negligent release of their health records.

The Court will dismiss the Wis. Stat. § 146.84(1)(bm) claims as to Plaintiffs Meza and Crosby, however. Both are alleged only to have provided *personal* information to OneTouchPoint pursuant to their employment. Because there are no allegations that OneTouchPoint had possession of any of Meza and Crosby's health records, their claims under the statute must be dismissed.

b. Plaintiffs Fail to Allege that OneTouchPoint Materially Induced a Pecuniary Loss, as Required by the Wisconsin Deceptive Trade Practices Act.

Plaintiffs next claim that OneTouchPoint also violated the Wisconsin Deceptive Trade Practices Act (WDTPA), Wis. Stat. § 100.18(1), by deceptively stating on its website that OneTouchPoint "maintain[s] commercially reasonable security measures to protect [Private Information] [it] collect[s] and store[s] from loss, misuse, destruction, or unauthorized access" and otherwise making false or misleading statements to the public. (ECF No. 15 ¶¶397–98.) To state a claim under the WDTPA, Plaintiffs must allege that: (1) OneTouchPoint made a representation to the public with the intent to induce an obligation; (2) that was untrue, deceptive, or misleading; and (3) materially induced a pecuniary loss to Plaintiffs. *See Hinrichs v. DOW Chemical Co.*, 937 N.W.2d 37, 56 (Wis. 2020).

OneTouchPoint first argues that the Consolidated Complaint fails to allege that OneTouchPoint made any misrepresentations regarding data security. (ECF No. 55-1 at 52.) This argument is inconsistent with Plaintiffs' pleadings. Plaintiffs specifically allege that OneTouchPoint made a representation, via its website, that it "maintain[s] commercially reasonable security measures to protect [Private Information] [it] collect[s] and store[s] from loss, misuse, destruction, or unauthorized access." (ECF No. 15 ¶397.) They further allege that this representation (along with others) was false deceptive, or misleading. (*Id.* ¶¶397–402.) Whether OneTouchPoint actually made those statements, and whether they were untrue, deceptive, or misleading, are fact questions inappropriate for resolution on a motion to dismiss.

OneTouchPoint's better argument is that any alleged misrepresentations were not directed to or received by Plaintiffs and thus could not have materially induced or caused Plaintiffs to suffer a loss. While a violation of Section 100.18(1) does not require that the plaintiff show that he or she reasonably relied on the defendant's misrepresentation, the plaintiff must show (or at this stage, plausibly allege) that the misrepresentation materially induced a pecuniary loss. The Consolidated Complaint does not plausibly allege such a causal connection between OneTouchPoint's alleged misrepresentations and any pecuniary loss by Plaintiffs. Plaintiffs point to allegations that several

of them would not have obtained health insurance or would not have accepted employment with OneTouchPoint if they had known OneTouchPoint "would negligently fail to adequately protect [their] private information." (ECF No. 59 at 39 (citing ECF No. 15 ¶¶264–65, 274–75, 284–85.) But those allegations are unrelated to OneTouchPoint's alleged misstatements. And Plaintiffs do not even suggest that the alleged misrepresentations were even directed to them. Nor do Plaintiffs allege that they were aware of the alleged misrepresentations. At most, Plaintiffs allege in conclusory fashion that they "reasonably relied upon [OneTouchPoint's] deceptive and unlawful marketing practices." (ECF No. 15 ¶405.) Such a conclusory allegation unsupported by plausible facts is insufficient even at the pleading stage. *See Fox*, 399 F. Supp. 3d at 798–99 ("Plaintiffs say that they 'believed the statements to be true and relied on them to their detriment,' . . . [b]ut these allegations are conclusory."). Accordingly, OneTouchPoint's motion to dismiss Plaintiffs' Wisconsin Deceptive Trade Practices Act claim will be granted.

2. Plaintiff Young Fails to State a Claim Under Maine Law

Plaintiffs also claim that OneTouchPoint violated the Maine Unfair Trade Practices Act (MUTPA), Me. Stat. tit. 5, § 205, *et seq.*, by failing to prevent the data breach, misrepresenting its data security, and failing to timely notify Young of the data breach. (ECF No. 15 ¶411.) This statute prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce," and provides a cause of action to "[a]ny person who purchases . . . goods, services or property . . . and thereby suffers any loss of money or property . . . as a result of the use or employment by another person" of any such unfair act. Me. Stat. tit. 5, §§ 207, 213(1). An act or practice is unfair if it (1) causes, or is likely to cause, substantial injury to consumers; (2) in not reasonably avoidable by consumers; and (3) is not outweighed by any countervailing benefits to consumers or competition. *State v. Weinschenk*, 868 A.2d 200, 206 (Me. 2005). "An act or practice is deceptive if it is a material representation, omission, act or practice that is likely to mislead consumers acting reasonably under the circumstances." *Id.*

OneTouchPoint argues that Young cannot recover under the Act because he was not a purchaser of OneTouchPoint's services, either directly or indirectly, has not alleged a "substantial" loss of money or property, and has not alleged any actual misrepresentations by OneTouchPoint concerning its data security. (ECF No. 55-1 at 54–56; ECF No. 62 at 23.) The Court will focus on OneTouchPoint's first argument. As Plaintiffs argue, the MUTPA allows for recovery to indirect purchasers. (ECF No. 59 at 41 (citing *Weinschenk*, 868 A.2d at 208).) But an indirect

purchaser must reasonably rely on the defendant's unfair practices, to their detriment, to recover under the MUTPA. *Weinschenk*, 868 A.2d 209 ("There is no evidence that the indirect purchasers relied on [the defendants'] misrepresentations or that the indirect purchasers sustained either a substantial injury or an ascertainable loss as a result of [the defendants'] misrepresentations."). Even if Young is an indirect purchaser of OneTouchPoint's services, he does not plausibly allege that he relied on any of OneTouchPoint's allegedly violative behavior in choosing to purchase medical services. Plaintiffs' conclusory allegation that Young "would not have obtained medical services from Martin's Point or Matrix . . . had he known that his healthcare provider's marketing service provider would negligently fail to adequately protect his PII/PHI," is insufficient even at the pleading stage. (*See* ECF No. 15 ¶297.) Plaintiffs offers no factual allegations plausibly suggesting that OneTouchPoint's allegedly unfair or deceptive practices had any impact on Young's actual behavior. The Consolidated Complaint does not allege that Young was even aware of OneTouchPoint, the services it provided to Matrix or Martin's Point, or its alleged unfair practices when making the decision to obtain medical services from Martin's Point. Thus, OneTouchPoint is correct that "Plaintiffs' argument stretches the 'indirect purchaser' theory beyond its limits." (ECF No. 62 at 23.) Regardless of whether Young was an indirect purchaser of OneTouchPoint's services, the Consolidated Complaints' non-conclusory allegations are insufficient to state a claim under the MUTPA.

3. Plaintiff Meza—a Former OneTouchPoint Employee—Cannot State a Claim Under the Arizona Consumer Fraud Act.

Plaintiffs further claim that OneTouchPoint violated the Arizona Consumer Fraud Act (ACFA) with respect to Meza by failing to prevent the data breach, misrepresenting its data security, failing to timely notify Meza of the data breach, and "omitting, suppressing, and concealing" its failure to comply with its statutory and common law duties and adequately protect Meza's data. (ECF No. 15 ¶434.) The ACFA "broadly prohibits fraudulent, deceptive or misleading conduct in connection with the sale or advertisement of consumer goods and services." *Cheatham v. ADT Corp.*, 161 F. Supp. 3d 815, 825 (D. Ariz. 2016) (citing Ariz. Rev. Stat. § 44-1522(A)). More specifically, the ACFA forbids the "act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise." Ariz. Rev. Stat. § 44-1522(A). It defines "merchandise" as

"any objects, wares, goods, commodities, intangibles, real estate or services." § 44-1521(5). Arizona courts construe the ACFA to provide a cause of action to any person damaged by a violation of the Act. *Cheatham*, 161 F. Supp. at 825 (citing *Sellinger v. Freeway Mobile Home Sales, Inc.*, 521 P.2d 1119, 1122 (Ariz. 1974)). "To prevail, a plaintiff must establish that (1) the defendant made a misrepresentation in violation of the Act, and (2) defendant's conduct proximately caused plaintiff to suffer damages." *Id.* (citing *Parks v. Macro-Dynamics, Inc.*, 591 P.2d 1005, 1008 (Ariz. Ct. App. 1979)). A misrepresentation causes injury only where the consumer actually relies on it. *Id.* at 825–26 (citing *Parks*, 591 P.2d at 1008). Rule 9(b)'s heightened pleading standard applies to claims under the Act. *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 53 (D. Ariz. 2021).

OneTouchPoint offers a host of arguments against Plaintiffs' ACFA claim. It contends that Plaintiffs fail to allege any actionable misrepresentation, that Meza was a consumer, and that any violation caused Meza's alleged injuries. (ECF No. 55-1 at 58–59.) OneTouchPoint also argues that Plaintiffs have not pleaded the ACFA claim with the specificity demanded by Rule 9(b). (*Id.* at 59.) Several of these arguments ring true and would likely justify dismissal of this claim. But the Court will focus on Plaintiffs' failure to allege that Meza was a consumer covered by the plain language of the ACFA. The Consolidated Complaint asserts that Meza was a previous employee of OneTouchPoint and provided his personal information to it in connection with that employment. (ECF No. 15 ¶¶208–09.) Because the parties' alleged relationship related to employment, it is not plausible that any misrepresentations or omissions OneTouchPoint made, as they pertain to Meza, would have been "in connection with the sale or advertisement of any merchandise," as required by the ACFA. *See* § 44-1522(A). Plaintiffs cite *Griffey.*, 562 F. Supp. 3d at 43, to support the viability of Meza's claim, but *Griffey* supports the Court's ruling here. (*See* ECF No. 59 at 45–46.) In *Griffey*, a group of plaintiffs that included employees sued following a data breach. 562 F. Supp. 3d at 41. The court dismissed all the plaintiffs' claims under the ACFA for failure to satisfy Rule 9(b). *Id.* at 53–54. In doing so, the court explained that dismissal of the employees' ACFA claims was also warranted because they were not consumers of the defendant's services as defined by the Act. *Id.* at 58–59 ("Plaintiffs . . . did not have a consumer-merchant relationship with [the defendant] because they were not the target of a sale or advertisement of health care services or data security."). This Court will likewise dismiss Meza's ACFA claim.

4. Plaintiff Meeks Has Stated a Claim Under Only Georgia's Fair Business Practices Act.

The Consolidated Complaint also asserts claims on behalf of Plaintiff Meeks under two Georgia statutes: the Security Breach Notification Act, Ga. Code Ann. § 10-1-912, and the Fair Business Practices Act, Ga. Code. Ann.§ 10-1-393(a). (ECF No. 15 ¶¶ 442–79.) OneTouchPoint seeks dismissal of both claims. For the following reasons, the Court will allow Meeks to proceed only on the second claim.

a. Georgia's Security Breach Notification Act Does Not Provide a Private Right of Action.

Plaintiffs claim that OneTouchPoint violated Georgia's Security Breach Notification Act (GSBNA) when it failed to disclose the breach to Meeks in a "timely and accurate manner." (ECF No. 15 ¶447.) The GSBNA requires businesses affected by a data breach to provide notice of the breach to Georgia residents "in the most expedient time possible and without unreasonable delay." § 10-1-912(a). OneTouchPoint challenges the viability of this claim, arguing that the statute does not provide a private right of action and, even if it did, Plaintiffs have not "adequately allege[d] a delay in notifying affected individuals" about the data breach. (ECF No. 55-1 at 59–60.)

In *In re Equifax, Inc., Customer Data Security Breach Litigation*, the District Court for the Northern District of Georgia concluded that the GSBNA does not provide a private right of action. 362 F. Supp. 3d 1295, 1342 (N.D. Ga. 2019) (citing *State Farm Mut. Auto. Ins. Co. v. Hernandez Auto Painting & Body Works, Inc.*, 719 S.E.2d 597, 601 (Ga. Ct. App. 2011)). It first noted that the GSBNA does not explicitly create a private right of action, *see* Ga. Code Ann. § 10-1-912, and emphasized that, under Georgia law, the absence of language creating a private right of action "strongly indicates the legislature's intention that no such cause of action be created by said statute." *Id.* (quoting *Hernandez Auto*, 719 S.E.2d at 601). Plaintiffs urge the Court not to follow *Equifax* and instead cite to *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1169–70 (D. Minn. 2014), in which the District Court for the District of Minnesota allowed a GSBNA claim to move forward. (ECF No. 59 at 46–47.) The Court will follow *Equifax*, not *Target*. The former case is from a federal court sitting in Georgia that is therefore more familiar with Georgia law. The latter case, in addition to being from a court with limited experience in Georgia law, largely turned on the parties' failure to provide evidence of how a court should interpret statutory silence as to enforcement under Georgia law. *See In re Target*, 66 F. Supp. 3d at 1170. The Court concludes there is no private right of action under the GSBNA.

Plaintiffs also argue that Ga. Code Ann. § 51-1-6, which states that "[w]hen the law requires a person to perform an act for the benefit of another or to refrain from doing an act which may injure another, although no cause of action is given in express terms, the injured party may recover for the breach of such legal duty if he suffers damage thereby," expressly authorizes recovery under the GSBNA. (ECF No. 59 at 47.) But Section 51-1-6 is Georgia's codification of negligence per se. *See Pulte Home v. Simerly*, 746 S.E.2d 173, 179 (Ga. Ct. App. 2013). While that statute might authorize recovery under a negligence theory for violation of a duty imposed by the GSBNA, the Consolidated Complaint pleads no such claim. Meeks's claim is for a violation of the GSBNA, not negligence or negligence per se, and the Consolidated Complaint contains no reference to Section 51-1-6. (*See* ECF No. 15 ¶442–49.) The Court will not credit Plaintiffs' attempt to indirectly replead their claim. Because there is not private right of action under the GSBNA, Meeks's claim under the statute must be dismissed.

b. Plaintiff Meeks Has Stated a Claim under the GFBPA.

Plaintiffs also claim that OneTouchPoint violated the Georgia Fair Business Practices Act (GFBPA) when it failed to prevent the data breach, misrepresented its data security, failed to timely notify Meeks of the data breach, and "omit[ed], suppress[ed], and conceal[ed]" its failure to comply with its statutory and common law duties and adequately protect Meeks's data. (ECF No. 15 ¶458.) The GFBPA makes unlawful "[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce." Ga. Code Ann. § 10-1-393(a). It provides a private right of action for any person "who suffers injury or damages . . . as a result of consumer acts or practices in violation of" the Act. *Id.* § 10-1-399(a).

OneTouchPoint argues that Meeks's claim fails because "there is no statutory basis for a duty to safeguard PII in Georgia, as the legislature has not enacted such a duty." (ECF No. 55-1 at 61 (citing *In re Equifax*, 362 F. Supp. 3d at 1329, 1338).) OneTouchPoint also argues that the Consolidated Complaint does not allege that it made any actual misrepresentations regarding its data security but supports this argument by stating only "[a]s discussed above" while failing to point the Court to any specific prior argument. (ECF No. 55-1 at 61; ECF No. 62 at 27.) Plaintiffs respond by asking the Court to credit an earlier decision from a district court in Georgia which allowed a GFBPA claim to proceed in a data breach case. (ECF No. 59 at 47–48 (citing *In re Arby's Rest. Grp. Inc. Litig.*, 317 F. Supp. 3d 1222, 1224–28 (N.D. Ga. 2018).) Plaintiffs also argue that Meeks's GFBPA claim does not rely solely on allegations that OneTouchPoint breached

a duty to protect his data, but also on allegations that OneTouchPoint affirmatively misrepresented that it would protect Meeks's private information, that it omitted material facts about its subpar security measures, and that it failed to timely and adequately notify Meeks following the breach. (*Id.* at 47 (citing ECF No. 15 ¶458).)

It is not necessary at this juncture for the Court to determine whether Georgia law creates a duty to safeguard private information. Plaintiffs are correct that Meeks's claim is not predicated solely on OneTouchPoint's failure to protect his information, but also on allegations that it misrepresented and omitted material information concerning its data security and the breach itself. (*See* ECF No. 15 ¶458(e)–(j).) OneTouchPoint challenges the sufficiency of these allegations only by commenting that the issue was discussed above, without directing the Court or Plaintiffs to where that discussion occurred or in what context. Moreover, the Court already concluded in its analysis of Plaintiffs' claim under the Wisconsin Deceptive Trade Practices Act that Plaintiffs have plausibly alleged that OneTouchPoint made one or more false or misleading statements concerning its data security. Thus, whether Georgia law requires OneTouchPoint to adhere to a certain standard of conduct concerning its data security practices or not, Plaintiffs have alleged misrepresentations by OneTouchPoint. And because OneTouchPoint does not otherwise challenge the sufficiency of Meeks's claim, he may proceed on his GFBPA claim.

5. Plaintiff Guertin Has Stated a Claim Under the South Carolina Data Breach Security Act.

Plaintiffs next claim that OneTouchPoint violated South Carolina's Data Breach Security Act when it failed to disclose the breach to Guertin in a "timely and accurate manner". (ECF No. 15 ¶533–40.) This statute requires that a person who "own[s] or licens[es]" data must disclose a data breach to any South Carolina resident whose data was compromised "in the most expedient time possible and without unreasonable delay." S.C. Code. Ann. § 39-1-90(A). The statute also explicitly creates a private cause of acting for both intentional and negligent violations of the statute. § 39-1-90(G)(1)–(2).

OneTouchPoint argues that Guertin's claim fails because Plaintiffs allege only in conclusory fashion that it owns or licenses data. OneTouchPoint cites *In re Blackbaud, Inc., Customer Data Breach Litigation*, in which a District of South Carolina court held that a conclusory assertion that the defendant "is a business owner that owns or licenses computerized data" was insufficient to state a claim under the Act. *Blackbaud*, No. 3:20-mn-02972-JMC, 2021

WL 3568394, at *16 (D.S.C. Aug. 12, 2021). But Plaintiffs argue that their allegations are slightly more detailed than those in *Blackbaud*. (*See* ECF No. 59 at 50.) The Consolidated Complaint alleges that OneTouchPoint "is contractually entitled to this information through its contracts with its healthcare and health insurance provider clients." (ECF No. ¶534.) OneTouchPoint responds that this is merely "[a]n additional conclusory allegation" and Plaintiffs fail to allege "how" OneTouchPoint is contractually entitled to Guertin's data. (ECF No. 62 at 29–30.)

The Court concludes that Plaintiffs have sufficiently alleged that OneTouchPoint owned or licensed Guertin's data, as required by the statute. Plaintiffs allege that OneTouchPoint's interest in Guertin's data stems from its "contracts with its healthcare and health insurance provider clients," to one of which (Humana) Guertin provided her data. (ECF No. 15 ¶¶249, 534.) This factual allegation provides more than the "formulaic recitation of the elements of a cause of action" that Rule 8 prohibits. *See Twombly*, 550 U.S. at 555 (citing *Papasan v. Allain*, 478 U.S. 265, 286 (1986)). OneTouchPoint cites to only *Blackbaud* in support of its argument for dismissal, but the court there contemplated a complaint that alleged only that the defendant "is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A)." *Blackbaud*, 2021 WL 3568394, at *16. In other words, the court dismissed because the complaint contained only a "formulaic recitation of the elements," which cannot survive a motion to dismiss. Plaintiffs do more here, if only just, and OneTouchPoint offers no support for its argument that their additional allegation is also insufficient. Mindful that a complaint "does not need detailed factual allegations" to survive a Rule 12(b)(6) motion to dismiss, *Twombly*, 550 U.S. at 555, the Court concludes that Plaintiffs have alleged just enough to create a plausible inference that OneTouchPoint "own[s] or licens[es]" Guertin's data.

OneTouchPoint also argues that the Consolidated Complaint "does not allege an unreasonable delay" and does not allege that OneTouchPoint violated the statute willfully, or that Guertin was actually injured by the violation. (ECF No. 55-1 at 65.) But the Consolidated Complaint alleges that OneTouchPoint did not notify Guertin of the breach until July 27, 2022, a full three months after the breach occurred. This significant delay is sufficient to create a plausible inference that OneTouchPoint failed to notify Guertin "in the most expedient time possible," as required by the statute. And contrary to OneTouchPoint's argument, the Consolidated Complaint does allege that Guertin was injured by the delay in notification. (*See* ECF No. 15 ¶14.)

Accordingly, Plaintiffs have stated a claim for violation of South Carolina's Data Breach Security Act on behalf of Guertin.

CONCLUSION

For the reasons detailed above, the Court concludes that Plaintiffs lack standing to sue for declaratory or injunctive relief, but all except Plaintiff Dusterhoft have standing, at this stage, to sue for damages. However, Plaintiffs have only stated claims for negligence, negligence per se, unjust enrichment (except Meza and Crosby) and violations of Wis. Stat. §§ 146.82(1), 146.84(1)(bm) (except Meza and Crosby), Georgia's Fair Business Practices Acts (Plaintiff Meeks), and South Carolina's Data Breach Security Act (Plaintiff Guertin). All other claims are dismissed.

IT IS HEREBY ORDERED that OneTouchPoint, Inc.'s Motion to Dismiss, ECF No. 55, is **GRANTED in part** and **DENIED in part**. All claims by Plaintiff Richard Dusterhoft and all Plaintiffs' claims for declaratory or injunctive relief are dismissed for lack of standing. Plaintiffs' common-law claims for breach of fiduciary duty, breach of third-party beneficiary contract, and breach of implied contract, as well as Meza's and Crosby's unjust enrichment claims, are dismissed for failure to state a claim. Plaintiff's claims under Wisconsin's Right to Privacy Act and Deceptive Trade Practices Act are also dismissed, as are Meza's and Crosby's claims under Wis. Stat. §§ 146.82(1), 146.84(1)(bm), Young's claims under the Maine Unfair Trade Practices and Uniform Deceptive Trade Practices Acts, Meza's claim under the Arizona Consumer Fraud Act, and Meeks's claims under the Georgia Security Breach Notification and Uniform Deceptive Trade Practices Acts. The balance of OneTouchPoint's motion is denied.

Dated at Milwaukee, Wisconsin on September 23, 2024.

s/ *Brett H. Ludwig*
BRETT H. LUDWIG
United States District Judge